|  |  |
| --- | --- |
|  | |
| МИНОБРНАУКИ РОССИИ | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** | |
| *(наименование института, филиала)* | |
| **Кафедра КБ-1 «Защита информации»** | |
| *(наименование кафедры)* | |

**ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ НА ПРОИЗВОДСТВЕННУЮ ПРАКТИКУ**

*(указать вид практики: учебная / производственная)*

**ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**

|  |
| --- |
| *(указать тип практики в соответствии с учебным планом)* |

|  |
| --- |
| **Студенту 3 курса учебной группы БББО-05-20**  Кутьину Захару Сергеевичу |
| *(фамилия, имя и отчество)* |

**Место и время практики:** Кафедра КБ-1 «Защита информации» 09.02.2023 – 31.05.2023

**Должность на практике (при наличии):** студент

**1. СОДЕРЖАНИЕ ПРАКТИКИ:**

1.1. Изучить: Принципы и средства мониторинга событий безопасности в сетях

1.2. Практически выполнить: Мониторинг событий безопасности в сетях малого бизнеса

1.3. Ознакомиться: с законодательством в области защиты информации, документами о малом бизнесе, статьями об угрозах и событиях безопасности в сетях

**2. Дополнительное задание:**  нет

**3. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ УКАЗАНИЯ:** Даны в устном виде. Оформление работы проводить в соответствии с рекомендациями по оформлению письменных работ в РТУ МИРЭА 2022/2023 гг

Руководитель практики от кафедры

|  |  |  |  |
| --- | --- | --- | --- |
| «09» февраля  2023 г. |  |  | (К.С. Щуров) |
|  | *Подпись* |  | *ФИО* |

Задание получил:

|  |  |  |  |
| --- | --- | --- | --- |
| «09» февраля  2023 г. |  |  | (З.С. Кутьин) |
|  | *Подпись* |  | *ФИО* |

**СОГЛАСОВАНО:**

И.о. заведующего кафедрой:

|  |  |  |  |
| --- | --- | --- | --- |
| «09» февраля  2023 г. |  |  | (С.В. Артёмова) |
|  | *Подпись* |  | *ФИО* |

**Проведенные инструктажи:**

|  |  |  |  |
| --- | --- | --- | --- |
| Охрана труда: | |  | «09» февраля 2023 г. |
|  | |  |  |
| Инструктирующий |  |  | (К.С. Щуров), доцент |
|  | *Подпись* |  | *Расшифровка, должность* |
| Инструктируемый |  |  | (З.С. Кутьин) |
|  | *Подпись* |  | *Расшифровка* |

|  |  |  |  |
| --- | --- | --- | --- |
| Техника безопасности: | |  | «09» февраля 2023 г. |
|  | |  |  |
| Инструктирующий |  |  | (К.С. Щуров), доцент |
|  | *Подпись* |  | *Расшифровка, должность* |
| Инструктируемый |  |  | (З.С. Кутьин) |
|  | *Подпись* |  | *Расшифровка* |

|  |  |  |  |
| --- | --- | --- | --- |
| Пожарная безопасность: | |  | «09» февраля 2023 г. |
|  | |  |  |
| Инструктирующий |  |  | (К.С. Щуров), доцент |
|  | *Подпись* |  | *Расшифровка, должность* |
| Инструктируемый |  |  | (З.С. Кутьин) |
|  | *Подпись* |  | *Расшифровка* |

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | «09» февраля 2023 г. |
|  | |  |  |
| Инструктирующий |  |  | (К.С. Щуров), доцент |
|  | *Подпись* |  | *Расшифровка, должность* |
| Инструктируемый |  |  | (З.С. Кутьин) |
|  | *Подпись* |  | *Расшифровка* |

|  |  |  |  |
| --- | --- | --- | --- |
| С правилами внутреннего распорядка ознакомлен: | |  | «09» февраля 2023 г. |
|  | |  |  |
|  |  |  | (З.С. Кутьин) |
|  | *Подпись* |  | *Расшифровка* |

|  |  |
| --- | --- |
|  | |
| |  | | --- | | МИНОБРНАУКИ РОССИИ | | Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| **Институт кибербезопасности и цифровых технологий (ИКБ)** | |
| *(наименование института, филиала)* | |
| **Кафедра КБ-1 «Защита информации»** | |
| *(наименование кафедры)* | |
| **ОТЧЁТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ**  *(указать вид практики: учебная / производственная)*  **ПРАКТИКА ПО ПОЛУЧЕНИЮ ПРОФЕССИОНАЛЬНЫХ УМЕНИЙ И ОПЫТА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ**  *(указать тип практики в соответствии с учебным планом)* | | |
|  | | |
| приказ Университета о направлении на практику от 16 января 2023 г. № 50-У | | |

|  |  |  |
| --- | --- | --- |
| Отчет представлен к рассмотрению: |  |  |
| Студент группы БББО-05-20 | «31» мая  2023 г. | /З.С. Кутьин |
|  |  | (подпись и расшифровка подписи) |
| Отчет утвержден. Допущен к защите: |  |  |
| Руководитель практики от кафедры | «31» мая  2023 г. | /К.С. Щуров |
|  |  | (подпись и расшифровка подписи) |

Москва 2023

|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |

**СОВМЕСТНЫЙ РАБОЧИЙ ГРАФИК**

**ПРОВЕДЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ**

студента Кутьина З.С. 3 курса группы БББО-05-20 очной формы обучения, обучающегося по направлению подготовки 10.03.01 «Информационная безопасность», профиль «Безопасность автоматизированных систем».

|  |  |  |  |
| --- | --- | --- | --- |
| **Неделя** | **Сроки выполнения** | **Этап** | **Отметка о выполнении** |
| 1-4 | 09.02.2023 - 09.03.2023 | Изучение предметной области | выполнено |
| 4-8 | ... | Написание теоретической части работы | выполнено |
| 8-12 | ... | Выполнение практической части работы | выполнено |
| 12-16 | ... - 31.05.2023 | Проверка руководителем практики | выполнено |

|  |  |  |
| --- | --- | --- |
| Руководитель практики от кафедры |  | / К.С. Щуров, доцент/ |
| Обучающийся |  | /З.С. Кутьин/ |

|  |  |  |
| --- | --- | --- |
| **Согласовано:** |  |  |
| И.о. заведующего кафедрой: |  | /С.В. Артёмова, д.т.н./ |

**Введение**

Ежегодно число кибератак на организации разных масштабов растет в 1,5 – 2 раза. Только в одном 2022 году число кибератак удвоилось и стало достигать 911 тыс. О таких данных «Ростелеком-Солар» рассказал 20 февраля 2023 года.

Также уже давно стали обычными новостями такие инциденты информационной безопасности как: утечки информации о кредитных картах, кража персональных данных, программы-вымогатели, кража интеллектуальной собственности, нарушение конфиденциальности, отказ в обслуживании, публикация в открытый доступ баз данных. Предприятия малого бизнеса не готовы выделять многомиллионные бюджеты на обеспечение своей безопасности, поскольку обладают достаточно ограниченными денежными и людскими средствами. Поэтому многие предприниматели обязаны знать несколько cредств мониторинга и контроля подключения к сети устройств, которые могут быть применимы в условиях ограниченных ресурсов.

В данной работе будет проведен анализ различных средств мониторинга и контроля подключения к стационарной сети устройств (точек WI-FI, АРМ, серверов и т.д.)

**1. Мониторинг и контроль подключения к сети**

**Мониторинг** – это непрерывный процесс наблюдения и регистрации различного рода событий. Это определение является простым объяснением понятия мониторинг.

**Мониторинг сети**, в свою очередь, – это процесс захвата, обработки и анализа пакетов данных, которые передаются или принимаются по компьютерной сети. Эти пакеты данных можно анализировать по различным показателям, таким как использование полосы пропускания, скорость потери пакетов, количество разорванных соединений и т. д.

По результатам проведенного анализа можно делать выводы о безопасности сети предприятия, что включает в себя выявление нарушителей, оценка уязвимостей сети, проверка надежности сети и др.

Существует несколько видов мониторинга сети. Рассмотрим некоторые из них, выберем самые актуальные и наиболее подходящие для предприятий малого бизнеса. Мониторинг подключения к TCP-порту

* Мониторинг ICMP (пинг);
* Мониторинг DNS-серверов;
* Мониторинг по протоколу ARP;
* Мониторинг SNMP (мониторинг значений MIB, OID, трафика и т.п.);
* Мониторинг порта на свитче (коммутаторе);
* Мониторинг состояния сетевого интерфейса/порта;
* Мониторинг FTP-серверов;
* Мониторинг HTTP-сервера (веб-сервера), мониторинг содержимого веб-страниц;
* Мониторинг MAC-адресов;
* Мониторинг выполнения JavaScript
* Мониторинг выполнения Visual Basic script
* Мониторинг баз данных: мониторинг MS SQL серверов, мониторинг MySQL-серверов, мониторинг серверов баз данных посредством ODBC
* Мониторинг параметров Linux, Unix через SSH по сети
* Объединение результатов проверок
* Вычисляемая по формуле проверка
* Мониторинг и учёт трафика с помощью NetFlow v5/9
* Мониторинг скорости трафика через SNMP
* Мониторинг почты e-mail (содержимое почтового ящика по протоколу POP3)
* Способы мониторинга систем и камер видеонаблюдения, IP-камер и видеорегистраторов (DVR или NVR) по сети
* Мониторинг OPC-сервера (OPC DA)
* Мониторинг уровня сигнала Wi-Fi
* Мониторинг QoS-метрик ICMP и UDP (jitter, MOS, задержка, потери, R-фактор)
* И др.

В наше время практически у любой организации или фирмы, даже самой маленькой, существует свой веб-сайт. Поэтому в современных реалиях большую актуальность имеют виды мониторинга, связанные с мониторингом данных циркулирующих в сети Интернет. Так же большую актуальность имеют виды мониторинга e-mail. Ведь вовремя проведенный анализ пакетов данных поступающих на e-mail сотрудника фирмы может спасти многие конфиденциальные данные как сотрудника, так и фирмы в целом.

Для того чтобы иметь возможность проводить сетевые исследования, необходимы так называемые сетевые протоколы или протоколы мониторинга.

Существует несколько различных протоколов, позволяющих проводить мониторинг. К некоторым из них относятся:

**1) Протокол SNMP**

Наиболее известным протоколом мониторинга является SNMP (Simple Network Management Protocol), который позволяет нам опрашивать компьютер и запрашивать у него различные значения. Например, количество переданных им байтов или температуру источника питания.

Эти значения идентифицируются цифровым кодом, называемым OID.

Например, OID для получения температуры источника питания в оборудовании CISCO выглядит следующим образом: 1.3.6.1.4.1.9.9.13.1.3.1.3

**2) Протокол ICMP**

Другим базовым протоколом является ICMP, который позволяет узнать, отвечает ли машина (широко известный как «отправка ping»).

Этот протокол также можно использовать для расчета времени задержки (сколько времени требуется пакету, чтобы добраться от одной машины к другой).

Определенные сетевые приложения, такие как IMAP, DNS или SMTP, имеют свои специфические порты, и знание того, работает ли служба должным образом, напрямую связано с дизайном протокола, поэтому необходимы более сложные тесты.

Как правило, любой сервис, предлагаемый по сети, открывает TCP-порт, поэтому мониторинг того, что эти порты активны и реагируют, уже может быть базовым мониторингом.

**2. Средства мониторинга. Типы и характеристики.**

Все многообразие средств, применяемых для мониторинга и анализа вычислительных сетей, можно разделить на несколько крупных классов:

* **Системы управления сетью (NetworkManagementSystems)** - централизованные программные системы, которые собирают данные о состоянии узлов и коммуникационных устройств сети, а также данные о трафике, циркулирующем в сети. Эти системы не только осуществляют мониторинг и анализ сети, но и выполняют в автоматическом или полуавтоматическом режиме действия по управлению сетью - включение и отключение портов устройств, изменение параметров мостов адресных таблиц мостов, коммутаторов и маршрутизаторов и т.п.
* **Средства управления системой (SystemManagement)** часто выполняют функции, аналогичные функциям систем управления, но по отношению к другим объектам. В первом случае объектом управления является программное и аппаратное обеспечение компьютеров сети, а во втором - коммуникационное оборудование.
* **Встроенные системы диагностики и управления (Embeddedsystems).** Эти системы выполняются в виде программно-аппаратных модулей, устанавливаемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в операционные системы. Они выполняют функции диагностики и управления только одним устройством, и в этом их основное отличие от централизованных систем управления.
* **Анализаторы протоколов (Protocolanalyzers).** Представляют собой программные или аппаратно-программные системы, которые ограничиваются в отличие от систем управления лишь функциями мониторинга и анализа трафика в сетях. Анализаторы протоколов позволяют установить некоторые логические условия для захвата отдельных пакетов и выполняют полное декодирование захваченных пакетов, то есть показывают в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга с расшифровкой содержания отдельных полей каждого пакета.
* **Оборудование для диагностики и сертификации кабельных систем.** Условно это оборудование можно поделить на четыре основные группы:
* Сетевые мониторы предназначены для тестирования кабелей различных категорий.
* Назначение устройств для сертификации кабельных систем, непосредственно следует из их названия. Сертификация выполняется в соответствии с требованиями одного из международных стандартов на кабельные системы.
* Кабельные сканеры используются для диагностики медных кабельных систем.
* Тестеры предназначены для проверки кабелей на отсутствие физического разрыва.
* **Экспертные системы.** Этот вид систем аккумулирует человеческие знания о выявлении причин аномальной работы сетей и возможных способах приведения сети в работоспособное состояние. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов.
* **Многофункциональные устройства анализа и диагностики.** В последние годы, в связи с повсеместным распространением локальных сетей возникла необходимость разработки недорогих портативных приборов, совмещающих функции нескольких устройств: анализаторов протоколов, кабельных сканеров и, даже, некоторых возможностей ПО сетевого управления.

Многие из представленных типов средств мониторинга являются либо слишком дорогими, что делает их недоступными для предприятий малого бизнеса, либо предоставляющий слишком широкий диапазон возможностей, наличие которых для малых предприятий просто излишне и сложно.

**3. Анализ средств мониторинга и контроля подключения к стационарной сети устройств**

Итак, что такое мониторинг и его важность в ИТ-системе теперь известно. Типы и свойства средств для мониторинга также рассмотрены. Осталось рассмотреть какие же существуют средства и провести анализ, выявить плюсы и минусы каждого из средств.

Очень важным преимуществом средства мониторинга сети будет его стоимость. Ведь предприятия малого бизнеса имеют небольшой бюджет и достаточно ограниченный набор ресурсов.

К счастью, на рынке сейчас доступно много хороших программ, как коммерческих, так и с открытым исходным кодом, способных наладить сетевой мониторинг.

Помимо цены, также важным фактором будет актуальность средства. Средство должно предоставлять достаточное количество и уровень возможностей для обеспечения потребностей предприятий малого бизнеса. Также средство должно иметь достаточный запас в обновлении, чтобы его актуальность сохранялась как можно дольше и поддерживалась на должном уровне безопасность сети.

Рассмотрим, какие программы для мониторинга сети являются самыми актуальными на сегодняшний день:

**Network Olympus.**

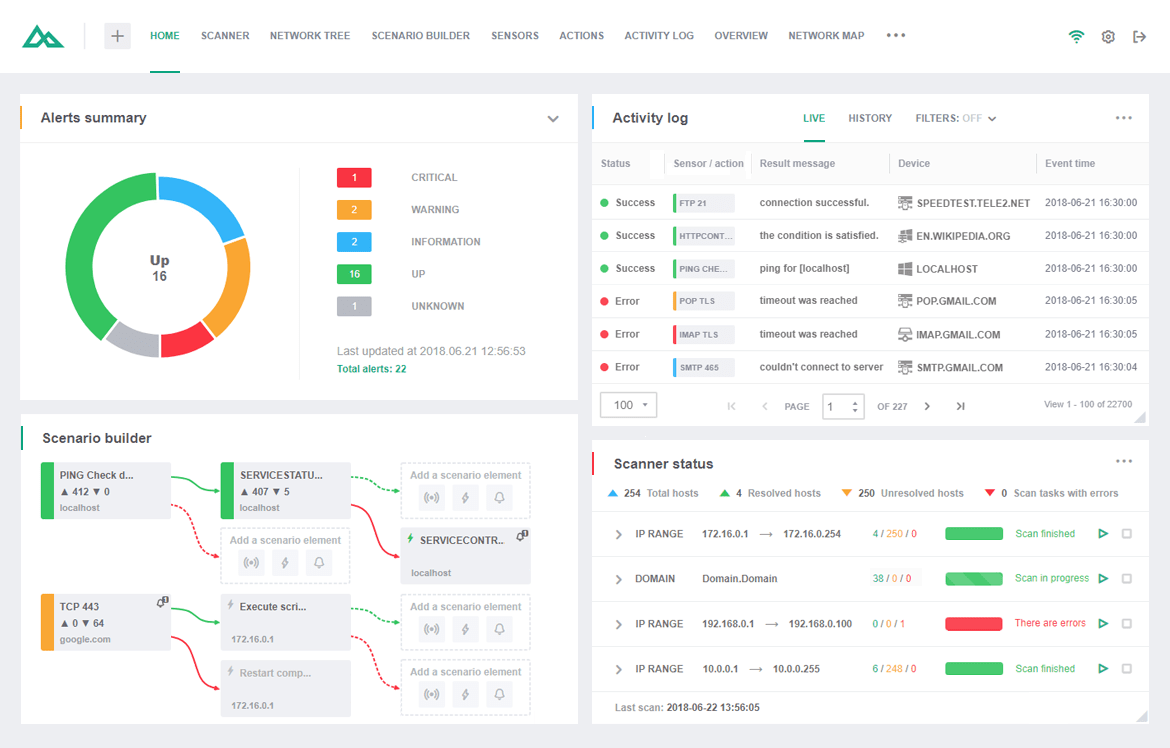


Рисунок 1 - Интерфейс Network Olympus.

Программа работает как служба и имеет веб-интерфейс, что дает гораздо большую гибкость и удобство в работе. Главная особенность – конструктор сценариев, позволяющий отойти от выполнения примитивных проверок, которые не позволяют учитывать те или иные обстоятельства работы устройств. С его помощью можно организовывать схемы мониторинга любой сложности, чтобы точно выявлять проблемы и неполадки, а также автоматизировать процесс их устранения.

В основе сценария лежит сенсор, от которого можно выстраивать логические цепочки, которые в зависимости от успешности проверки будут генерировать разные оповещения и действия, направленные на решение различных задач. Каждый элемент цепочки может быть отредактирован в любое время и сразу применится для всех устройств, за которыми закреплен сценарий. Вся сетевая активность будет отслеживаться при помощи журнала активности и специальных отчетов.

**Observium.**

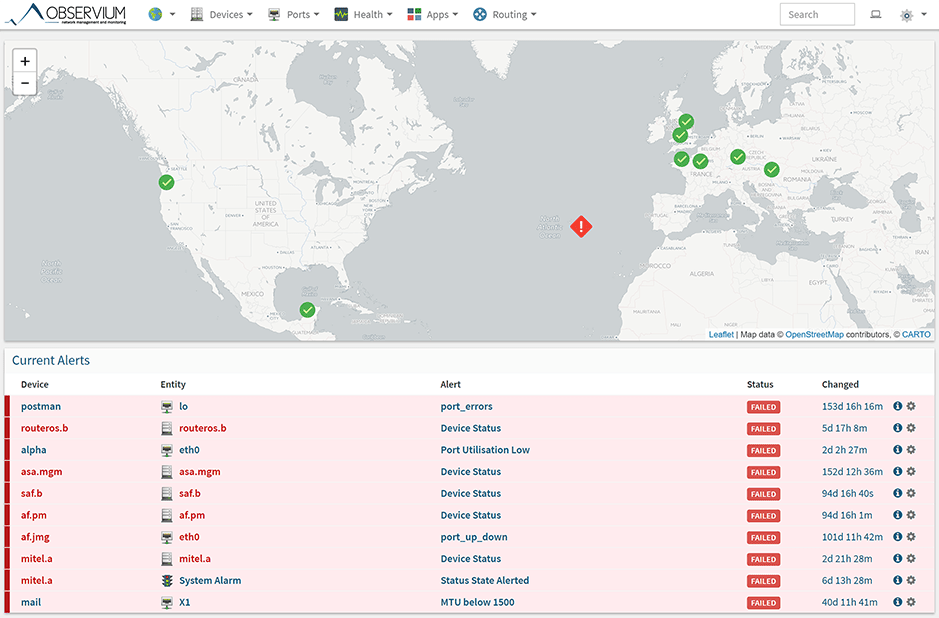


Рисунок 2 - Интерфейс Observium.

Приложение Observium, работа которого основана на использовании протокола SNMP, позволяет не только исследовать состояние сети любого масштаба в режиме реального времени, но и анализировать уровень ее производительности. Это решение интегрируется с оборудованием от Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp и прочих вендоров. Благодаря идеально проработанному графическому интерфейсу, данное ПО предоставляет системным администраторам массу вариантов для настройки – начиная от диапазонов для автообнаружения и заканчивая данными протокола SNMP, необходимыми для сбора информации о сети.

Также они получают доступ к данным о технических характеристиках всего оборудования, которое в текущий момент подключено к сети. Все отчеты, которые формируются посредством анализа журнала событий, Observium может представлять в виде диаграмм и графиков, наглядно демонстрируя "слабые" стороны сети.

**Nagios.**

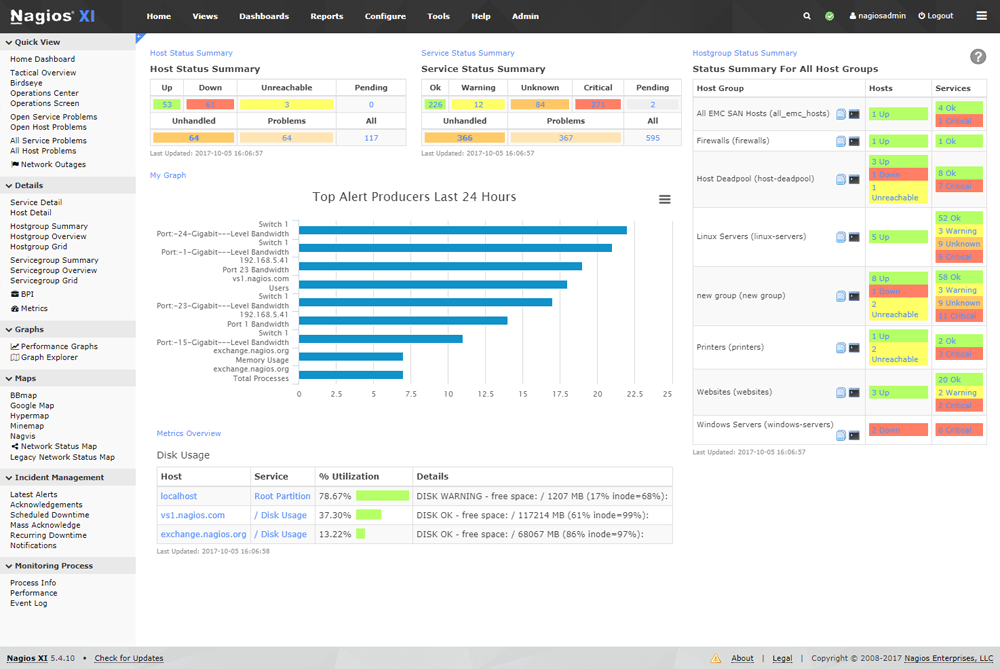


Рисунок 3 - Интерфейс Nagios.

Nagios – это продвинутое решение для мониторинга, управление которым основано на веб-интерфейсе. Он отнюдь не прост в освоении, однако, благодаря своему довольно большому интернет-сообществу и хорошо проработанной документации, может быть освоен за несколько недель.

С помощью Nagios системные администраторы получают возможность удаленно регулировать объем нагрузки на пользовательское или вышестоящее в сетевой иерархии оборудование (коммутаторы, маршрутизаторы, серверы), следить за степенью загруженности резервов памяти в базах данных, следить за физическими показателями частей сетевого оборудования (например, температурой материнской платы, сгорание которой является одной из самых частых поломок в данной сфере) и пр.

Nagios автоматически отправляет тревожные уведомления на предустановленный сисадмином адрес – будь то адрес электронной почты или номер телефона мобильного оператора.

**PRTG Network Monitor.**

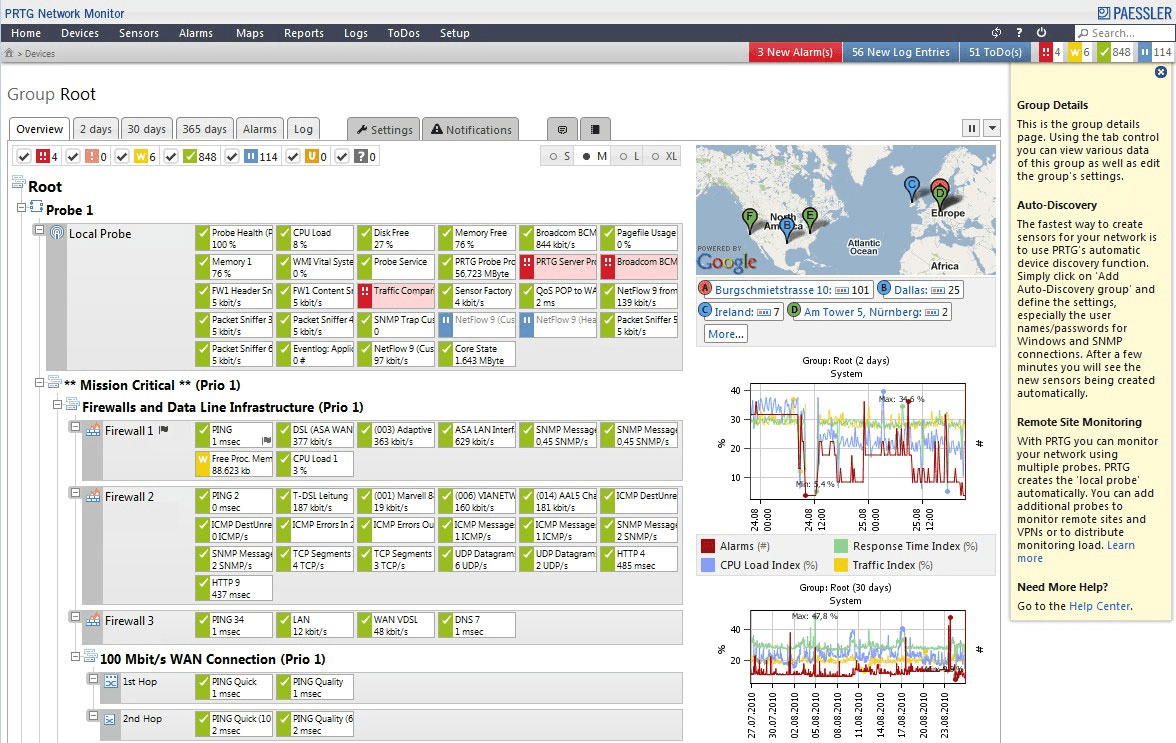


Рисунок 4 - Интерфейс PRTG Network Monitor.

Программный компонент PRTG, совместимый с устройствами на базе ОС Windows, предназначен для мониторинга сетей. Он используется не только для сканирования устройств, которые в данный момент подключены к локальной сети, и может послужить отличным помощником в обнаружении сетевых атак.

Среди самых полезных сетевых сервисов PRTG: инспекция пакетов, анализ и сохранение статистических данных в базу, просмотр карты сети в режиме реального времени (также доступна возможность получения исторических сведений о поведении сети), сбор технических параметров об устройствах, подключенных к сети, а также анализ уровня нагрузки на сетевое оборудование. Он очень удобен в использовании – прежде всего, благодаря интуитивно понятному графическому интерфейсу, который открывается при помощи любого браузера. В случае необходимости, системный администратор может получить и удаленный доступ к приложению, через веб-сервер.

**Kismet.**

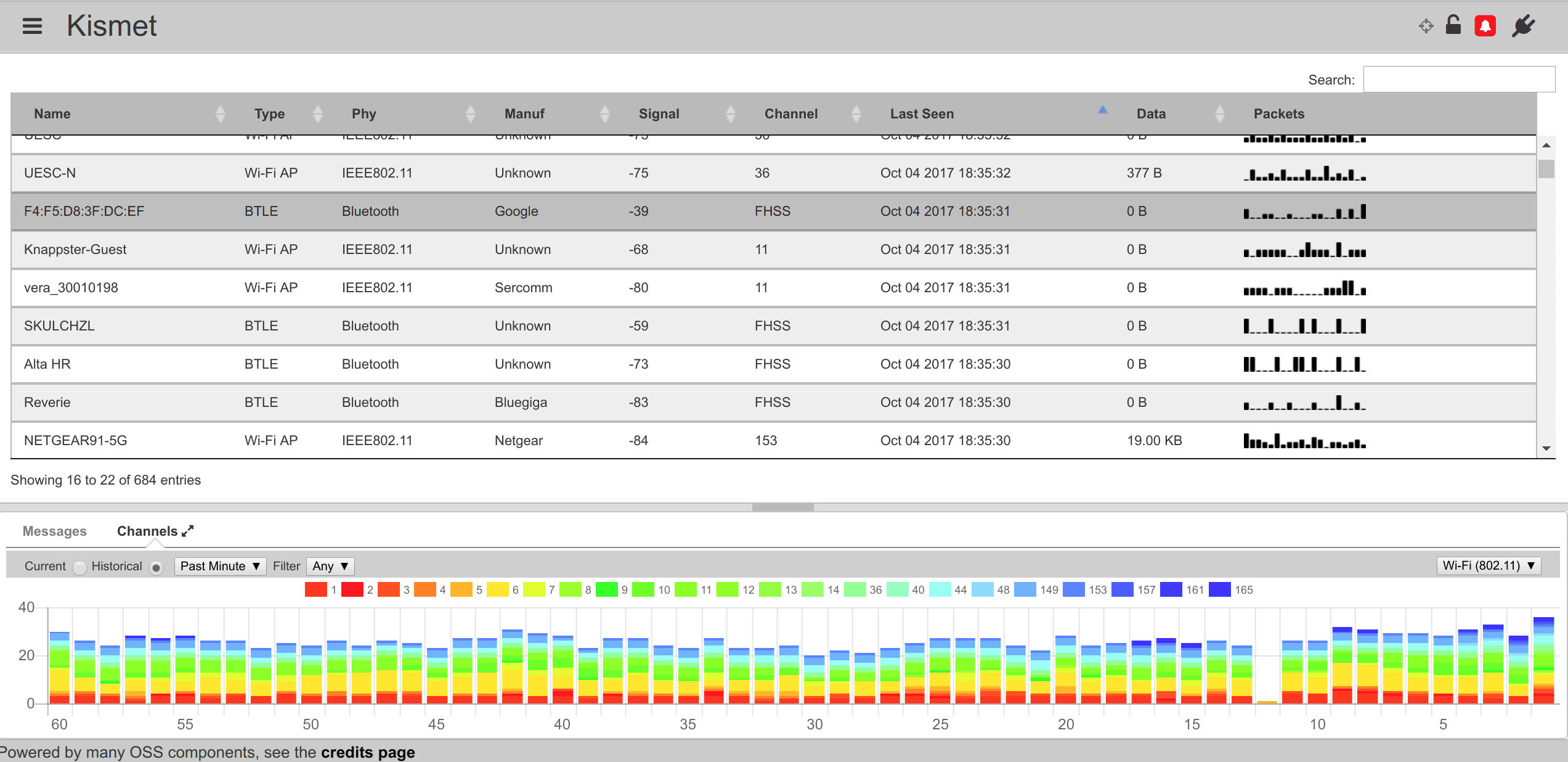


Рисунок 5 - Инфтерфейс Kismet.

Kismet – это полезное open-source приложение для системных администраторов, которое позволяет всесторонне анализировать сетевой трафик, обнаруживать в нем аномалии, предотвращать сбои и может быть использовано с системами на базе \*NIX/Windows/Cygwin/macOS. Kismet нередко используется именно для анализа беспроводных локальных сетей на основе стандарта 802.11 b.

С его помощью без труда возможно найдти некорректно сконфигурированные и даже нелегально работающие точки доступа (которые злоумышленники используют для перехвата трафика) и прочие скрытые устройства, которые могут быть потенциально "вредны" для сети. Для этих целей в приложении очень хорошо проработана возможность обнаружения различных типов сетевых атак – как на уровне сети, так и на уровне каналов связи. Как только одна или несколько атак будут обнаружены, системный администратор получит тревожный сигнал и сможет предпринять меры по устранению угрозы.

**WireShark.**

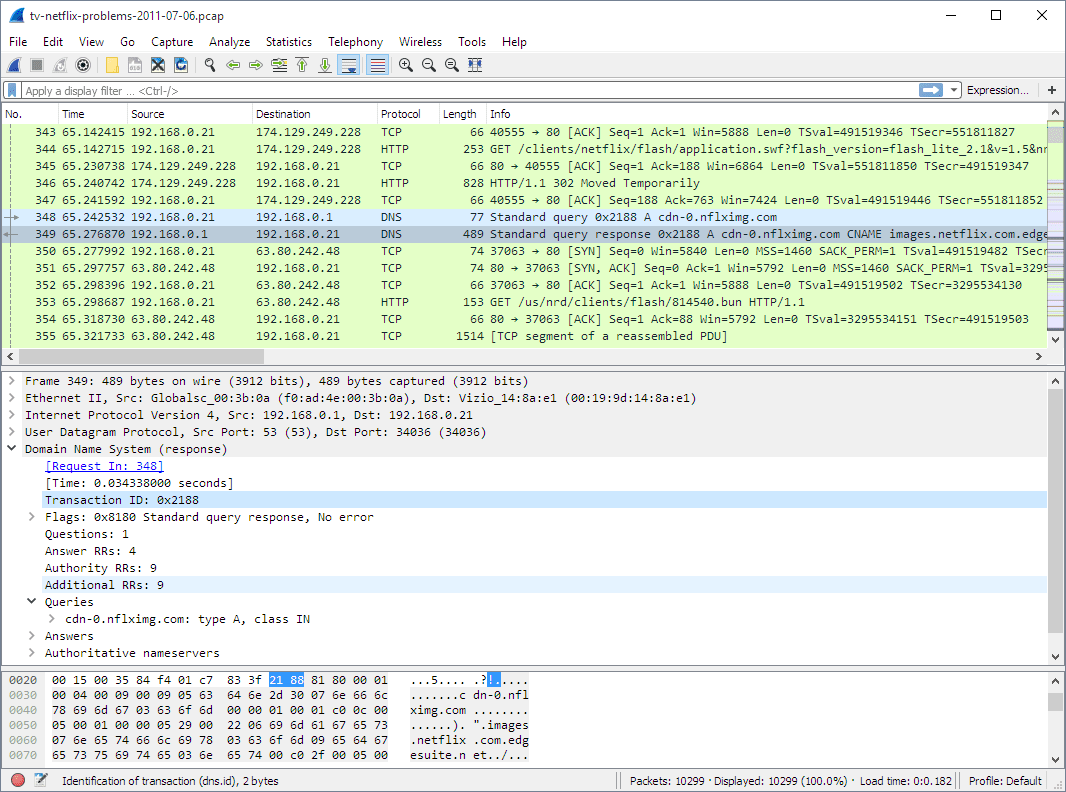


Рисунок 6 - Интерфейс WireShark.

Бесплатный open-source анализатор трафика WireShark предоставляет своим пользователям невероятно продвинутый функционал и по праву признан образцовым решением в области сетевой диагностики. Он идеально интегрируется с системами на базе \*NIX/Windows/macOS.

Вместо не слишком хорошо понятных для новичков веб-интерфейсов и CLI, в которых нужно вводить запросы на специальном программном языке, данное решение использует GUI.

После разворачивания и настройки его единожды на сервере, получается централизованный элемент для мониторинга за мельчайшими изменениями в работе сети и сетевых протоколах.

**NeDi.**

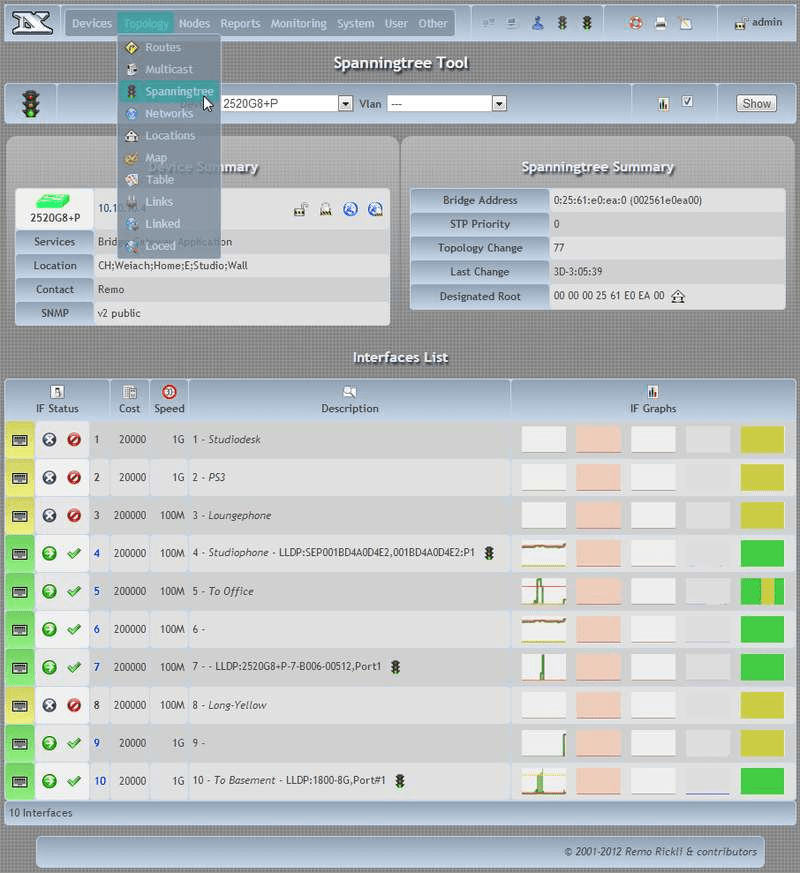


Рисунок 7 – Интерфейс NeDi.

NeDi – это полностью бесплатное ПО, которое сканирует сеть по MAC-адресам (также среди допустимых критериев поиска есть IP-адреса и DNS) и составляет из них собственную БД. Для работы этот программный продукт использует веб-интерфейс.

Таким образом, возможно в режиме онлайн наблюдать за всеми физическими устройствами и их местоположением в рамках локальной сети.

Некоторые профессионалы задействуют NeDi для поиска устройств, которые используются нелегально (например, украдены). Для подключения к коммутаторам или маршрутизаторам данное ПО использует протоколы CDP/LLDP. Это очень полезное, хотя и непростое в освоении решение.

**Zabbix.**

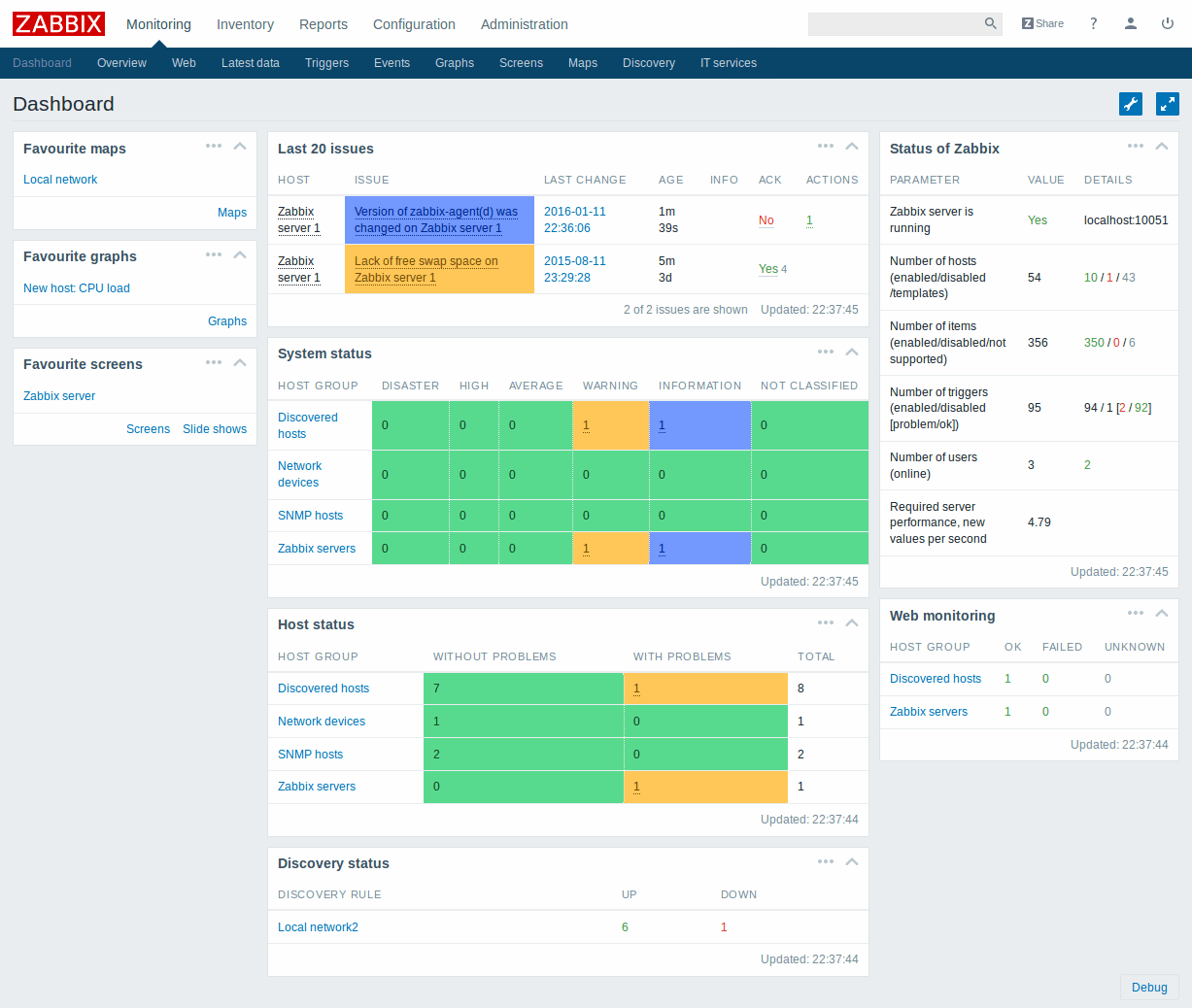


Рисунок 8 - Интерфейс Zabbix.

Система мониторинга Zabbix – это универсальное решение для сетевого мониторинга с открытым исходным кодом, которое может быть сконфигурировано под отдельные сетевые модели. В основном, оно предназначено для систем, которые обладают многосерверной архитектурой (в частности, Zabbix интегрируется с серверами Linux/FreeBSD/Windows).

Данное приложение позволяет одновременно управлять сотнями сетевых узлов, что делает его крайне эффективным инструментом в организации работы сисадминов, работающих на крупномасштабных предприятиях. Для развертывания Zabbix в локальной сети потребуется либо запустить программных агентов (демонов), либо использовать SNMP-протокол (или другой протокол для защищенного удаленного доступа); а для управления придется освоить веб-интерфейс на PHP

Кроме того, это ПО предоставляет полноценный набор инструментов для отслеживания состояния аппаратной части сети. Для того, чтобы в полной мере ощутить все преимущества данного решения, необходимо обладать хотя бы базовыми знаниями языков Perl или Python.

**10-Страйк: Мониторинг Сети.**

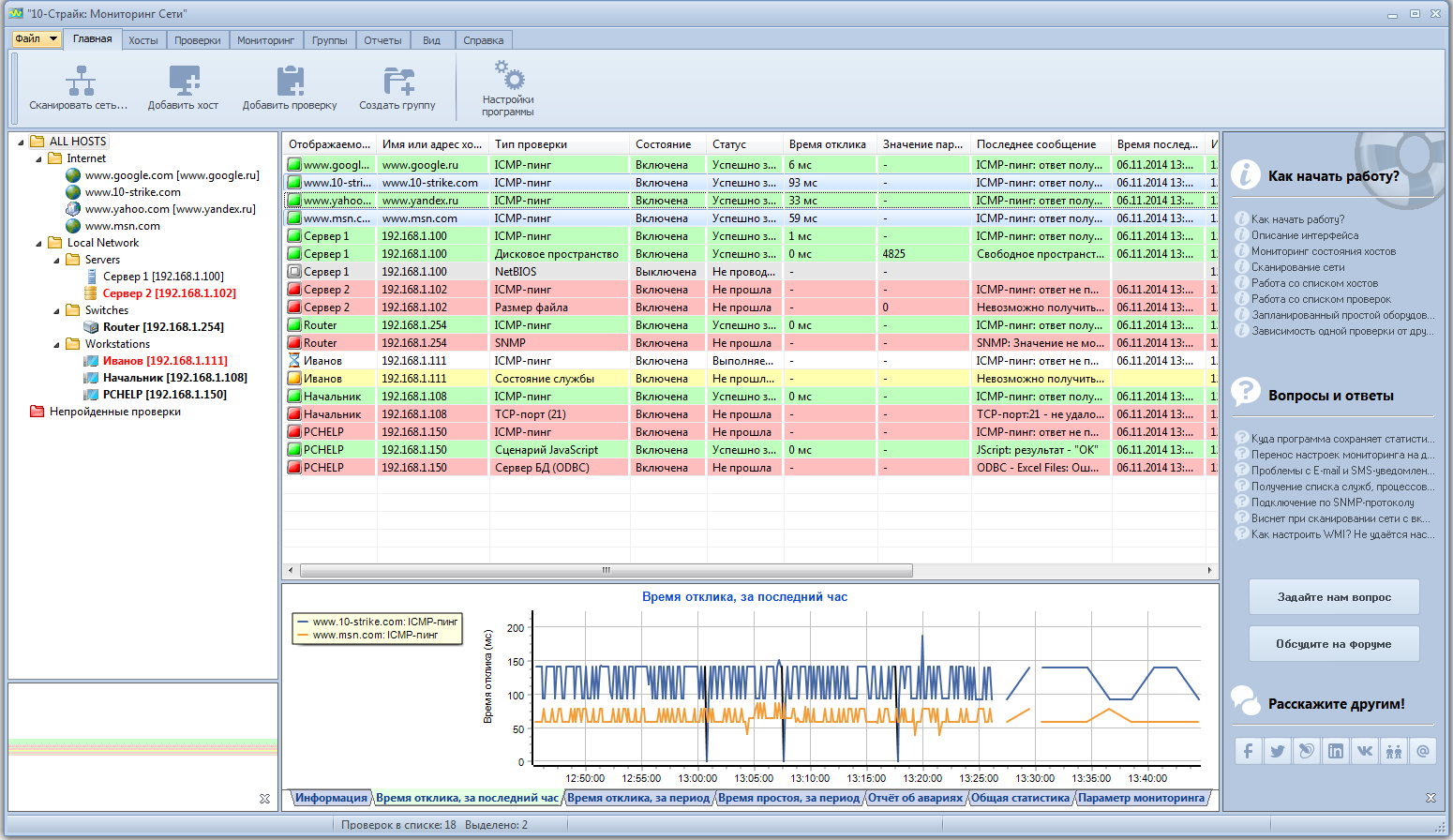


Рисунок 9 - Интерфейс 10-Срайк: Мониторинг Сети.

"Мониторинг сети" – это программное решение на базе веб-интерфейса, которое полностью автоматизирует все аспекты сетевой безопасности. С его помощью системные администраторы могут предотвращать распространение по локальной сети вирусного ПО, а также определять причину возникновения всевозможных технических неисправностей, связанных с разрывом кабелей или выходом из строя отдельных единиц сетевой инфраструктуры.

Кроме того, данное программное обеспечение в режиме онлайн выполняет мониторинг температуры, напряжения, места на дисках и прочих параметров по SNMP и WMI.

**Total Network Monitor 2.**

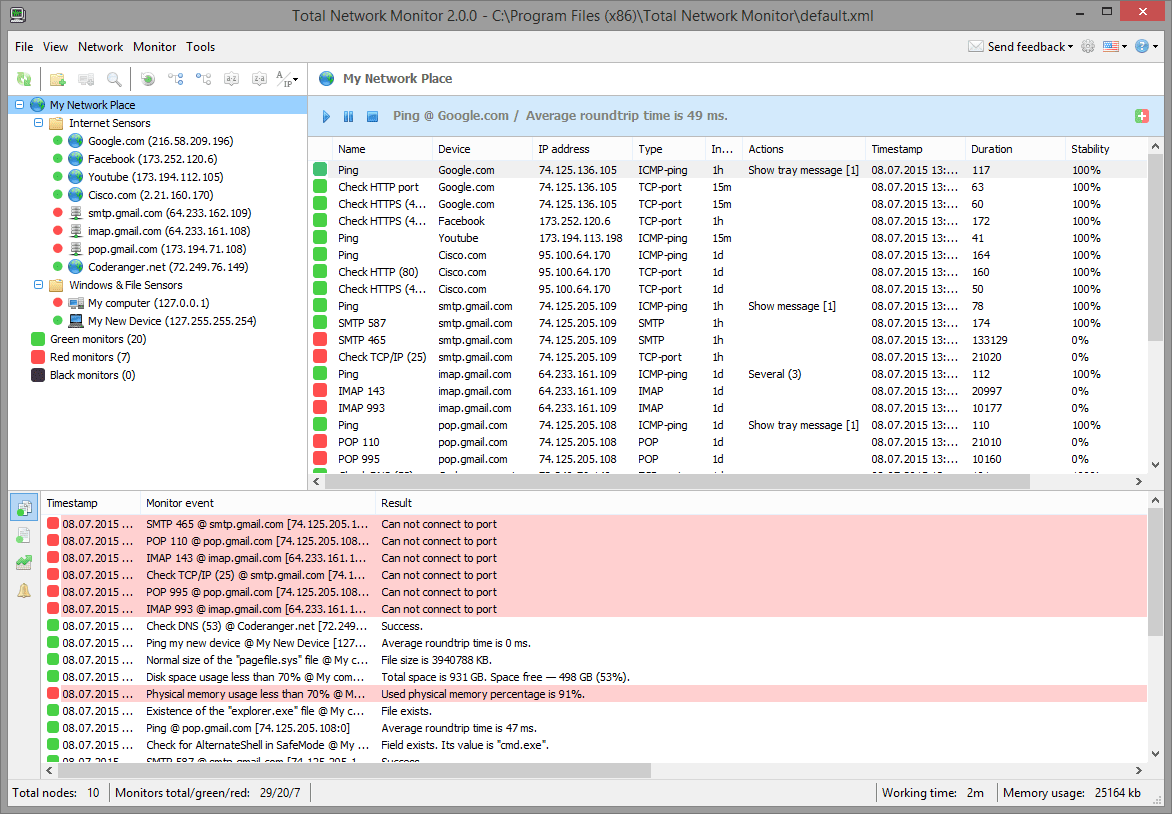


Рисунок 10 - Интерфейс Total Network Monitor 2.

Total Network Monitor 2 – крайне доступное и действенное программное решение для сетевого мониторинга, которое имеет идеальный баланс между удобством (в большинстве бесплатных решений отсутствует GUI) и функционалом. Одним из основных настраиваемых компонентов TNM 2 являются мониторы, которые выполняют проверки с необходимой периодичностью. Они позволяют отследить практически любой параметр, начиная от доступности серверов в сети и заканчивая проверкой состояния сервисов.

Ниже в таблице представлены все преимущества и недостатки рассмотренных средств мониторинга сети с общей точки зрения.

Таблица 1 – Преимущества и недостатки средств мониторинга сети.

|  |  |  |
| --- | --- | --- |
| **Средства** | **Преимущества** | **Недостатки** |
| Network Olympus | Групповые сенсоры;  Простота настройки;  Прост в освоении;  Конструктор сценариев мониторинга; | Только веб-интерфейс;  Установка только под Windows;  Нет многопользовательского доступа; |
| Observium | Доступна бесплатная версия;  «Пороговые» сигналы;  Функции автоматического обнаружения;  Доступна для многих систем; | Нет поддержки мобильных устройств;  Сложна в установке;  Для маленьких сетей;  Недостатки бесплатной версии; |
| Nagios | Высокая гибкость;  Полезные шаблоны;  Интеграция с другими приложениями; | Трудоемкая настройка; |
| PRTG Network Monitor | Множество функций;  Настраиваемые панели;  Гибкий мониторинг;  Карта сети; | Высокая цена;  Нет отдельной базы данных;  Нет групповых сенсоров; |
| Kismet | Бесплатна;  Пакетный сниффер;  Минималистичный интерфейс; | Сложна в использовании;  Медленный сканер;  Трудно обучиться; |
| WireShark | Бесплатна;  Проста в установке;  Анализатор пакетов;  Гибкий интерфейс; | Не интуитивна;  Нет мобильной поддержки; |
| NeDi | Бесплатна;  Множество возможностей;  Отличная карта сети; | Только для macOS;  Трудно установить;  Трудно обучиться; |
| Zabbix | Бесплатна;  Проста в установке;  Множество плагинов;  Мощные настройки оповещений; | Нет версии для Windows;  Сложный громоздкий интерфейс  Высокая нагрузка на компьютер; |
| 10-Страйк: Мониторинг Сети | Удобный и простой интерфейс; | Относительно дорогая;  Требовательна к системе; |
| Total Network Monitor 2 | Низкая цена;  Легко установить;  Дружественный интерфейс; | Нет многопоточности;  Не обновляется; |

**Вывод**

Для небольших компаний нужно универсальное решение за разумную стоимость, простотой установки и управления, которое позволит гибко настроить использование ресурсов компании, а так же обеспечит комплексную защиту от всех типов угроз, чтобы вопросы информационной безопасности не отходили на задний план.

Однозначно выбрать и назвать лучшую программу мониторинга сети трудно. Но по проведенному анализу можно придерживаться мнения, что Network Olympus обладает многими достоинствами и очень низким порогом входа, ведь он не требует специального обучения для того, чтобы начать с ним работать. Кроме того, ему не свойственны недостатки open-source решений, такие как отсутствие обновлений и плохая совместимость (как с ОС, так и с ТХ устройств).

Таким образом, благодаря подобному решению возможно контролировать все события, происходящие в пределах сети и своевременно на них реагировать.